LISP Data-Plane Cryptography

draft-ietf-lisp-crypto-02

LISP Working Group - Yokohama IETF
October 2015

Dino Farinacci & Brian Weis
Document Status

• WG draft -00 created Jan 2015, presented in Dallas spring 2015

• WG draft -01 created May 2015, presented in Prague summer 2015

• WG draft -02 created Sep 2015, presented here in Yokohama fall 2015
Design Summary

- Diffie-Hellman exchange via Map-Request/Map-Reply
- Keys not stored by third-party
- Keys are ephemeral
- ITR $\text{encrypt-n-encap}$ -> ETR $\text{decap-n-decrypt}$
- Rekeying part of RLOC-probing
- Cipher suite negotiation for AEAD
  - AES and Chacha20 ciphers
  - SHA1/Poly1305 HMACs
Changes to -02

Cipher Suite 4:
Difference in Name: 256-bit Elliptic-Curve 25519 [CURVE25519]
Encryption: AES with 128-bit keys in CBC mode [AES-CBC]
Integrity: HMAC-SHA1-96 [RFC2404]

Cipher Suite 5:
Difference in Name: 256-bit Elliptic-Curve 25519 [CURVE25519]
Encryption: Chacha20 [CHACHA-POLY]
Integrity: Poly1305 [CHACHA-POLY] (i.e. AEAD_CHACHA20_POLY1305)
Implementation Status

• *lispers.net* has a -02 implementation

<table>
<thead>
<tr>
<th>Cipher Suite 1:</th>
</tr>
</thead>
<tbody>
<tr>
<td>Diffie-Hellman Group: 1024-bit Modular Exponential (MODP) [RFC2409]</td>
</tr>
<tr>
<td>Encryption: AES with 128-bit keys in CBC mode [AES-CBC]</td>
</tr>
<tr>
<td>Integrity: HMAC-SHA1-96 [RFC2404]</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Cipher Suite 4:</th>
</tr>
</thead>
<tbody>
<tr>
<td>Diffie-Hellman Group: 256-bit Elliptic-Curve 25519 [CURVE25519]</td>
</tr>
<tr>
<td>Encryption: AES with 128-bit keys in CBC mode [AES-CBC]</td>
</tr>
<tr>
<td>Integrity: HMAC-SHA1-96 [RFC2404]</td>
</tr>
</tbody>
</table>

• Uses ECDH instead of regular DH:
  • RFC5114 gx value from the “192-bit Random ECP Group”
  • Added Curve25519

• Supports rekeying via RLOC-probing

• Support for unidirectional encryption across NATs
  • RTR to xTR-behind NAT as well as xTR-behind-NAT to RTR
Chacha20 vs AES

Look at “crypto-time” below in microseconds.

With AES for 1000-byte packets:

With CHACHA for 1000-byte packets:
Chacha20 for 100-byte pings

dino-macbook-> egrep chacha-time logs/lisp-etra.log
09/23/15 11:00:15.695: etr: Decrypt for key-id: 1, RLOC: 130.211.169.66, ICV: 0xa62db19...b82810a7 (good),
   chacha-time: 581 usec
09/23/15 11:00:16.697: etr: Decrypt for key-id: 1, RLOC: 130.211.169.66, ICV: 0xa12a04a3...e715570e (good),
   chacha-time: 454 usec
09/23/15 11:00:17.703: etr: Decrypt for key-id: 1, RLOC: 130.211.169.66, ICV: 0x0bd6943f...78c7802d (good),
   chacha-time: 266 usec
09/23/15 11:00:18.709: etr: Decrypt for key-id: 1, RLOC: 130.211.169.66, ICV: 0xbaf0d1e7...724a05e2 (good),
   chacha-time: 513 usec
09/23/15 11:00:19.712: etr: Decrypt for key-id: 1, RLOC: 130.211.169.66, ICV: 0xdc2e7319...e600549c (good),
   chacha-time: 498 usec
09/23/15 11:00:20.720: etr: Decrypt for key-id: 1, RLOC: 130.211.169.66, ICV: 0x261b62f2...f237501d (good),
   chacha-time: 725 usec
09/23/15 11:00:21.723: etr: Decrypt for key-id: 1, RLOC: 130.211.169.66, ICV: 0x40298619...24bb57c5 (good),
   chacha-time: 527 usec
09/23/15 11:00:22.728: etr: Decrypt for key-id: 1, RLOC: 130.211.169.66, ICV: 0x3b3c2335...fc678639 (good),
   chacha-time: 370 usec
09/23/15 11:00:23.740: etr: Decrypt for key-id: 1, RLOC: 130.211.169.66, ICV: 0x98f2750d...848992f9 (good),
   chacha-time: 383 usec
09/23/15 11:00:24.744: etr: Decrypt for key-id: 1, RLOC: 130.211.169.66, ICV: 0xd2b3454c...0564cc06 (good),
   chacha-time: 380 usec
09/23/15 11:00:25.661: etr: Decrypt for key-id: 1, RLOC: 130.211.169.66, ICV: 0xcc64e190...de1feb61 (good),
   chacha-time: 380 usec
09/23/15 11:00:26.660: etr: Decrypt for key-id: 1, RLOC: 130.211.169.66, ICV: 0xa51d9200...d0f9f0e0 (good),
   chacha-time: 368 usec
09/23/15 11:00:27.671: etr: Decrypt for key-id: 1, RLOC: 130.211.169.66, ICV: 0x3265f7e...045f0060 (good),
   chacha-time: 485 usec
09/23/15 11:00:28.680: etr: Decrypt for key-id: 1, RLOC: 130.211.169.66, ICV: 0x3557f03...70eb07df (good),
   chacha-time: 380 usec
09/23/15 11:00:29.688: etr: Decrypt for key-id: 1, RLOC: 130.211.169.66, ICV: 0x01c6ab42...e1253f0c (good),
   chacha-time: 372 usec
09/23/15 11:00:30.697: etr: Decrypt for key-id: 1, RLOC: 130.211.169.66, ICV: 0x4892c6cc...1e2d15c9 (good),
   chacha-time: 401 usec
09/23/15 11:00:31.705: etr: Decrypt for key-id: 1, RLOC: 130.211.169.66, ICV: 0x90ae1e34...9fbd11c8 (good),
   chacha-time: 380 usec
09/23/15 11:00:32.711: etr: Decrypt for key-id: 1, RLOC: 130.211.169.66, ICV: 0x7db401c8...d63c3003 (good),
   chacha-time: 250 usec
09/23/15 11:00:33.719: etr: Decrypt for key-id: 1, RLOC: 130.211.169.66, ICV: 0x8ef531d4...dbb6d5d5 (good),
   chacha-time: 370 usec
09/23/15 11:00:34.729: etr: Decrypt for key-id: 1, RLOC: 130.211.169.66, ICV: 0x3092e67...2fe1789 (good),
   chacha-time: 313 usec
09/23/15 11:00:35.736: etr: Decrypt for key-id: 1, RLOC: 130.211.169.66, ICV: 0xd3b45543...b86b0c74 (good),
   chacha-time: 377 usec
09/23/15 11:00:36.748: etr: Decrypt for key-id: 1, RLOC: 130.211.169.66, ICV: 0x69d5154f...aad0ab5f (good),
   chacha-time: 380 usec
Implementation Todo List

• Key Related Testing
  • Larger keys, other ECDH groups, and other ciphers
  • Multi-key rekeying logic

• Multi-Feature Testing
  • Test multicast in unicast encapsulation
  • Test with LISP-SEC

• Interoperability Testing
  • Making a call for more implementations
  • How about lispmob and open source the code?
Questions?